

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-366525

(43)Date of publication of application : 20.12.2002

(51)Int.Cl.

G06F 15/00

(21)Application number : 2001-215975

(71)Applicant : NEEDS CREATOR KK

(22)Date of filing : 12.06.2001

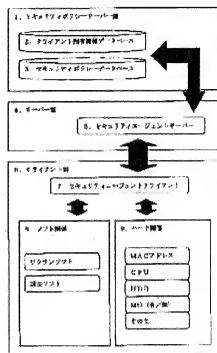
(72)Inventor : KOSHIDA TOSHIO

(54) SECURITY POLICY MAINTENANCE SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To newly develop a system for maintaining the security policy of a network.

SOLUTION: When a client 6 logs in a network, resource information of the client is acquired by a security agent client 7, transmitted to a security agent server 5, an information data base 2 intrinsic to the client is compared with a security policy data base 3 in a security policy server 1 and permission or nonpermission of network log in by the client 6 is determined. In addition, the security agent client 7 always monitors an operating state of the client 6, transmits it to the security agent server 5 and when breach of the security policy is caused, disconnects network connection by the client 6.



(19)日本西特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-366525

(P2002-366525A)

(43)公開日 平成14年12月20日 (2002.12.20)

(51)Int.Cl. ⁷	識別記号	F I	テームド(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 D 5 B 0 5 5
	3 2 0		8 2 0 K

審査請求 未請求 請求項の数 3 書面 (全 4 頁)

(21)出願番号 特願2001-215975(P2001-215975)

(71)出願人 501082338

ニーズクリエイター株式会社

福岡県福岡市中央区苅町1丁目21番11号

(22)出願日 平成13年6月12日 (2001.6.12)

(72)発明者 越田 敏江

福岡県福岡市中央区苅町1丁目21-11 ニーズクリエイター株式会社内

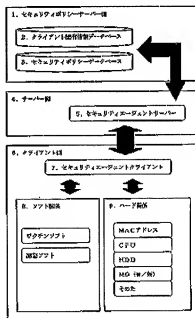
フターム(参考) 58085 AC01 AC11 AE00 BM07 EC07

(54)【発明の名称】 セキュリティポリシー維持システム

(57)【要約】

【課題】ネットワークのセキュリティポリシーを維持するシステムが無かった

【解決手段】6のクライアントがネットワークにログインする際に、7のセキュリティエージェントクライアントにて、クライアントのリソース情報を取得し、5のセキュリティエージェントサーバーに送信され、1のセキュリティポリシーサーバー内の、2のクライアント固有情報データベースと3のセキュリティポリシーデータベースと比較し、8のクライアントのネットワークログイン許可または不許可を判断する。また、7のセキュリティエージェントクライアントは、常時8のクライアントの動作状況を監視し、5のセキュリティエージェントサーバーに送信し、セキュリティポリシー違反が発生した場合、8のクライアントのネットワーク接続を切断する。



(2)

特開2002-368525

1

【特許請求の範囲】

【請求項1】 ネットワークに参加するクライアントのセキュリティレベルにより、サーバー側よりクライアントのネットワーク参加を許可および拒否する手段と、前記のセキュリティレベル情報を取得し、クライアントとサーバー間でセキュリティレベルの照会手段と、備えたことを特徴とする、セキュリティポリシー維持管理装置やアプリケーションとそれを記録する媒体

【請求項2】 クライアントがネットワークに参加し、遠隔を継続している間も、クライアントのセキュリティレベル情報を監視し、セキュリティレベルがネットワーク参加可能レベルより低くなった場合やセキュリティレベル情報の取得が出来なくなった場合にネットワーク資源の利用を制限する手段とを備えたことを特徴とする、メール管理装置やアプリケーションとそれを記録する媒体

【請求項3】 ネットワーク管理者が許可した正規クライアントと無許可のクライアントの判断手段とを備えたことを特徴とする、セキュリティポリシー維持管理装置やアプリケーションとそれを記録する媒体

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、コンピュータネットワークの利用においてネットワークに参加するクライアントセキュリティレベルにより、ネットワークセキュリティレベル管理制御装置やアプリケーションとそれを記録する媒体に関するものである。

【0002】

【従来の技術】 従来は、コンピュータネットワークを構築し運用していく場合は、事前に運用マニュアル等を作成し、その中でセキュリティ維持のための項目を設定し、利用者のモラルの向上を行い、セキュリティレベルを維持していた。

【0003】 また、ネットワーク参加者の区別は、ネットワークログインIDとパスワードのみチェックで参加を許可していた為、プライベートパソコンを取り扱ったセキュリティレベルを維持していないクライアントも、簡単にネットワークに参加していた。

【0004】 また、ネットワーク管理者が知らないセキュリティレベルの低いクライアントが数多くネットワークに参加する事で、ネットワークのセキュリティレベルが低下し、ウイルスへの感染や情報の漏洩などの重大な問題が発生する場合があった。

【0005】

【発明が解決しようとする課題】 本発明は、前記の課題を解決する為に、クライアントのセキュリティレベル情報を取得し取得したセキュリティレベルによりネットワークへの参加を拒否および制限を行うことが出来る様にしたもので、以下の効果および方法を特徴とする。

【0006】 本発明の目的は、ネットワーク管理者が定

2

めたセキュリティレベルの基準に至らないクライアントのネットワーク参加を制限する管理方法を提供することにある。

【0007】

【課題を解決するための手段】 サーバーとクライアントにセキュリティチェックエージェントを常駐させ、クライアントの電源を入れ、起動した時点からセキュリティエージェントが起動する。そのセキュリティエージェントは、クライアント上にネットワーク管理者が設定した、当時正常動作に必要なアプリケーションの稼働状況とバージョン情報の取得を行う。また、その他の稼働中アプリケーション情報の取得を行い、取得した情報をログイン処理と共にサーバーに伝送する。

【0008】 サーバー側は、伝送されたクライアントセキュリティ情報および、クライアントのMACアドレスやCPUおよびHDDサイズ等の固有データをセキュリティポリシー設定データベースの内容と比較し、ネットワーク参加の可否を判断する。

【0009】 ネットワーク参加が許可された場合は、ネットワーク資源を利用する事が出来る様になるが、不許可の場合は、ネットワークログインを拒否する。

【0010】 また、前記のセキュリティエージェントが稼働していないクライアントからネットワークサーバーにログイン処理が行われた場合は、サーバー側に常駐しているセキュリティエージェントにより、ネットワークログイン処理を強制的に中断し、ネットワーク参加を拒否する。

【0011】

【発明の實施の形態】 ネットワーク利用者は、自己の管理している6のクライアントを起動し、起動後IDとパスワードを入力して、ネットワークにログインする。

【0012】 前記のクライアントが、正規許可のクライアント場合は、7のセキュリティエージェントクライアントにより、8のソフト稼働状況や9のハードリソース情報が取得され、ログイン処理と共に7のセキュリティエージェントクライアントから5のセキュリティエージェントサーバーに送られ、6のセキュリティエージェントサーバーは、1のセキュリティポリシーデータベース上の、2のクライアント固有情報データベースと3のセキュリティポリシーデータベース情報を元に、ログインの可否を判断する。

【0013】 セキュリティレベルが基準に達していれば、5のセキュリティエージェントサーバーは、7のセキュリティエージェントクライアントに対し、ログインを許可する。

【0014】 しかし、セキュリティレベルが基準以下の場合は、5のセキュリティエージェントサーバーは、7のセキュリティエージェントクライアントに対し、ログインを拒否し、ログインの拒否理由を7のセキュリティエージェントクライアントに送返する。7のセキュリティ

(3)

特開 2002-368525

3

エージェントクライアントは、受取した拒否理由を表示する。利用者は指示に従って対処し、再度ログイン処理を行う。

【0015】また、個人所有の正規許可のクライアントが無い場合は、7のセキュリティエージェントクライアントが稼動しているか、または稼動していてもMACアドレスやCPUおよびHDDサイズなどのクライアント固有の情報が、2のクライアント固有情報データベースに登録が無い為、5のセキュリティエージェントサーバにより、ネットワーク参加が拒否される。

【0016】また、7のセキュリティエージェントクライアントは、ネットワークに接続中に、6のクライアントのソフトやハードのリソースに変化を検出し、5のセキュリティエージェントサーバに通知する、5のセキュリティエージェントサーバは、通知内容がセキュリティポリシーデータベースと比較し、セキュリティポリシーに違反があれば、6のクライアントをネットワークより強制的に切断する。

【0017】また、5のセキュリティエージェントサーバは、常時7のセキュリティエージェントクライアントの動作を監視し、7のセキュリティエージェントクライアントからの信号が途絶えた場合、6のクライアントのセキュリティレベルに異常が発生したと判断し、ネッ

4

＊ネットワークより強制的に切断する。

【0018】

【発明の効果】本発明のセキュリティポリシー維持システムを利用する事で、セキュリティポリシーに違反するクライアントの接続を防止し、ネットワークのセキュリティレベルを維持できる。また、各クライアントのリソース状況をデータベースに登録し管理することで、悪意を持ってMOやRAS環境開設を行っても、ネットワークから自動的に切り離される為、機密情報や個人情報情報の漏洩やウィルスの侵入を防止することができる。

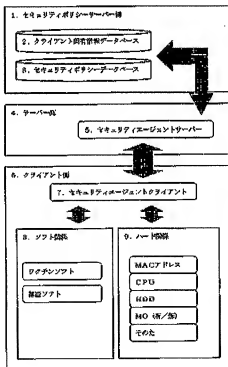
【図面の簡単な説明】

【図1】本発明の基本処理の流れを説明した図である

【符号の説明】

- 1 - セキュリティポリシーサーバ
- 2 - クライアント固有情報データベース
- 3 - セキュリティポリシーデータベース
- 4 - サーバ側
- 5 - セキュリティエージェントサーバ
- 6 - クライアント
- 7 - セキュリティエージェントクライアント
- 8 - ソフト関係
- 9 - ハード関係

【図1】



(4)

特開2002-366525

【手続補正書】

【提出日】平成13年7月23日(2001. 7. 23)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】請求項2

【補正方法】変更

【補正内容】

【請求項2】 クライアントがネットワークに参加し、
 処理を継続している間も、クライアントのセキュリティ
 レベル情報を監視し、セキュリティレベルがネットワー
 ク参加可能レベルより低くなった場合セキュリティレ
 ベル情報の取得が出来なくなった場合にネットワーク資
 源の利用を制限する手段とを備えたことを特徴とする、

セキュリティポリシー維持管理装置やアプリケーション
 とそれを記録する媒体

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】発明の属する技術分野

【補正方法】変更

【補正内容】

【発明の属する技術分野】本発明は、コンピュータネッ
 トワークの利用においてネットワークに参加するクライ
 アントセキュリティレベルにより、ネットワーク参加を
制限する装置やアプリケーションとそれを記録する媒体
 に関するものである。